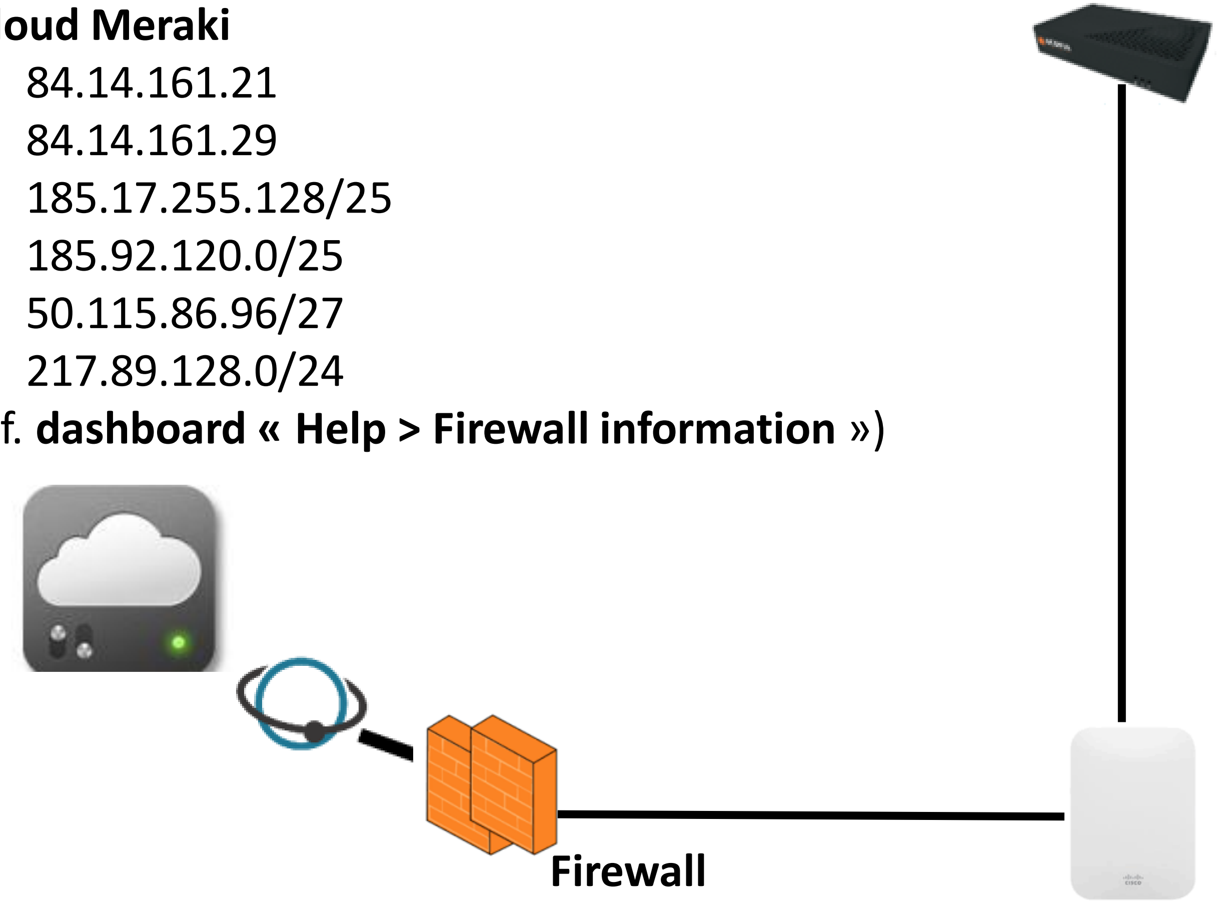
UCOPIA

TURN YOUR WI-FI UP

Out-Of-Band Meraki

UCOPIA Communications

CONTEXT



Cloud Meraki

- 84.14.161.21
- 84.14.161.29
- 185.17.255.128/25
- 185.92.120.0/25
- 50.115.86.96/27
- 217.89.128.0/24

(cf. **dashboard « Help > Firewall information** »)

Central UCOPIA
172.16.10.150
cloud1.ucopia.com

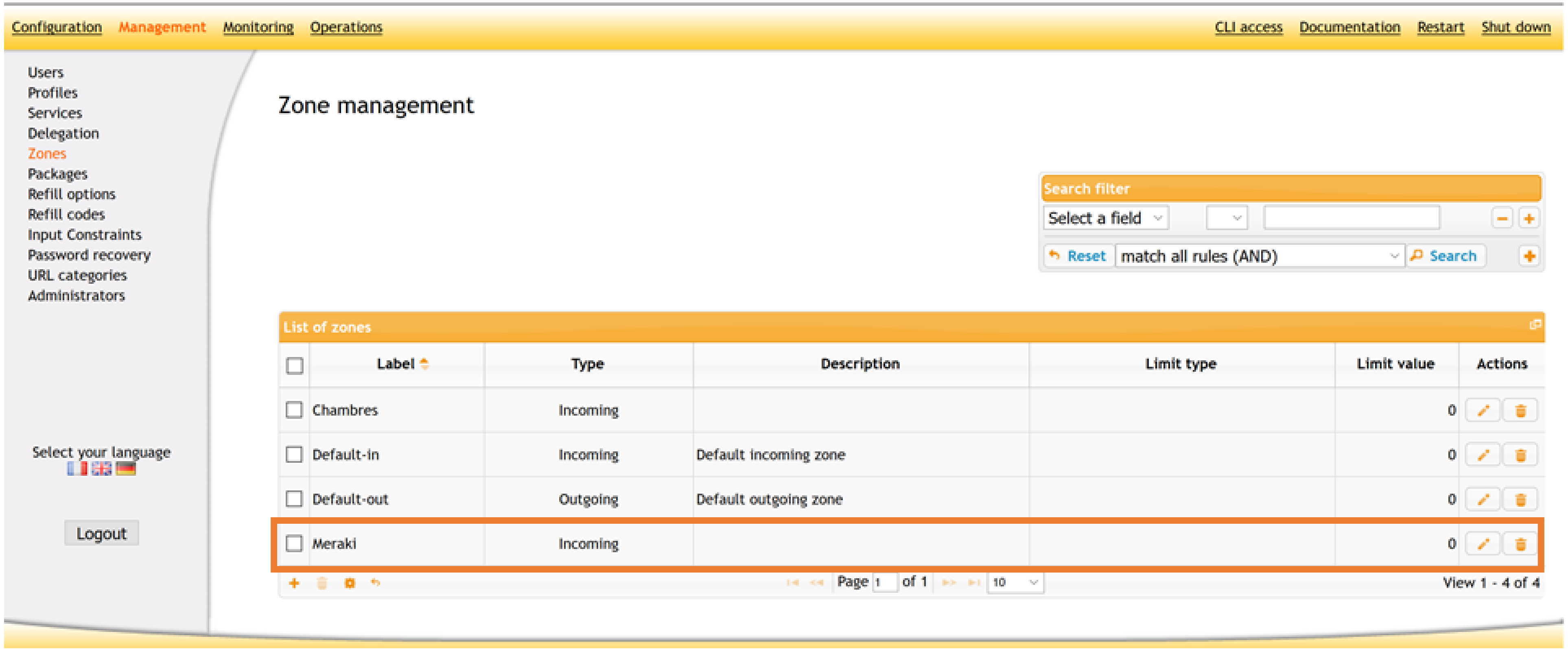
Meraki AP
10.0.1.111 (DHCP)

Firewall
10.0.0.1

→ Correct FW openings rules need to be applied so that Meraki AP can communicate with Cloud Meraki

UCOPIA CONFIGURATION

Create the concerned zone (e.g. « Meraki »)



Zone management

match all rules (AND)

List of zones

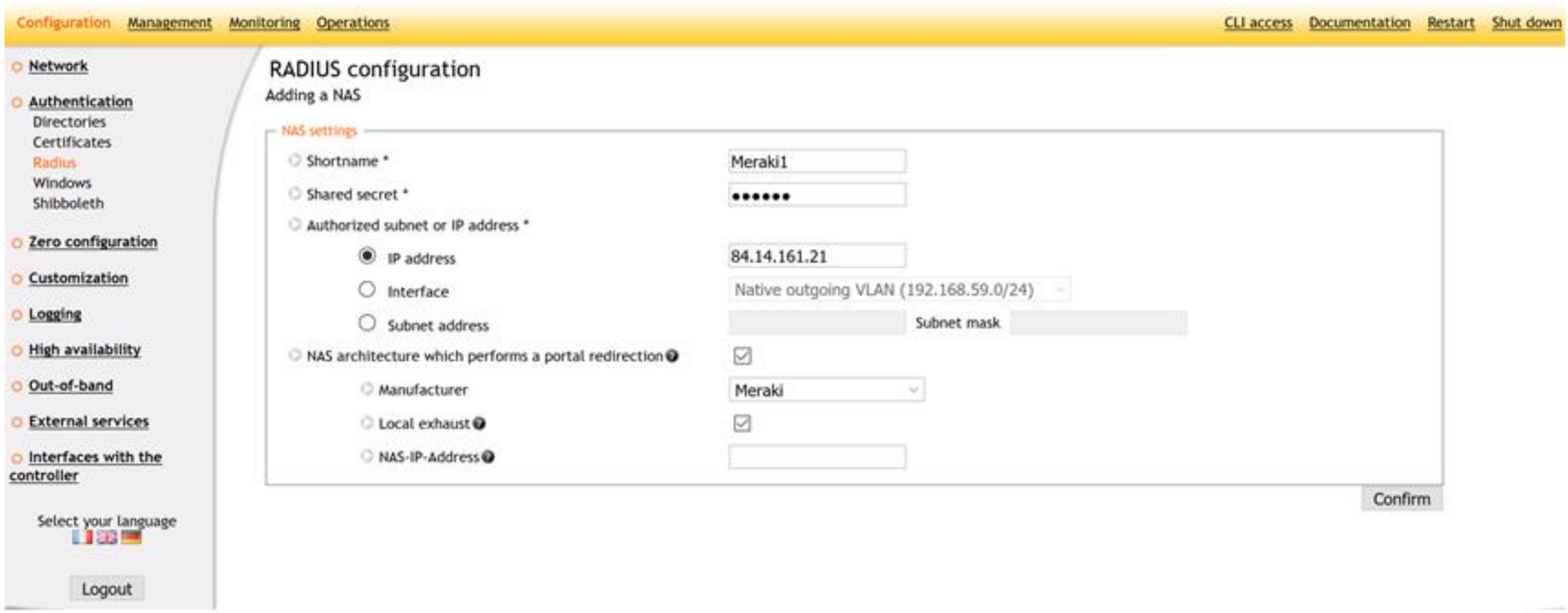
□	Label	Type	Description	Limit type	Limit value	Actions
□	Chambres	Incoming			0	
□	Default-in	Incoming	Default incoming zone		0	
□	Default-out	Outgoing	Default outgoing zone		0	
□	Meraki	Incoming			0	

View 1 - 4 of 4

UCOPIA CONFIGURATION

Create as many NAS configuration in the central UCOPIA as needed for the inbound traffic:

- 84.14.161.21
- 84.14.161.29
- 185.17.255.128/25
- 185.92.120.0/25
- 50.115.86.96/27
- 217.89.128.0/24



RADIUS configuration

Adding a NAS

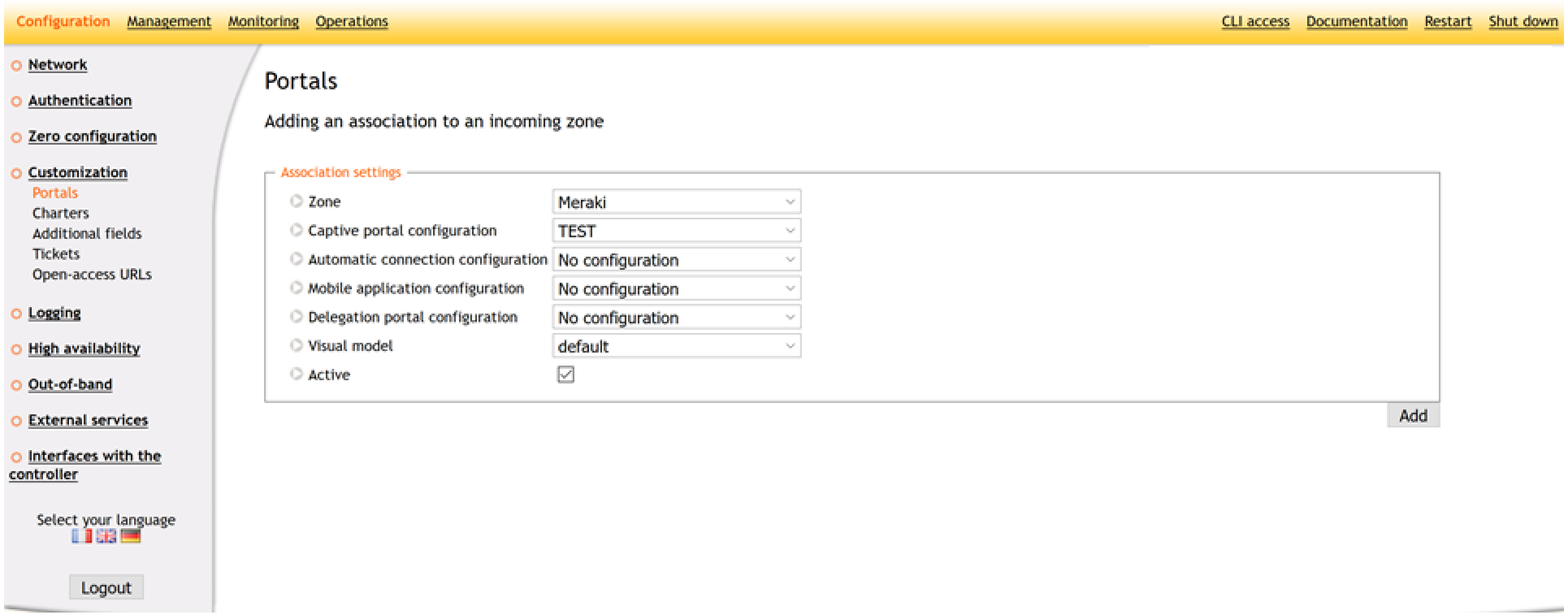
NAS settings

Shortname *	Meraki1
Shared secret *	••••••
Authorized subnet or IP address *	
● IP address	84.14.161.21
○ Interface	Native outgoing VLAN (192.168.59.0/24)
○ Subnet address	Subnet mask
NAS architecture which performs a portal redirection	☑
Manufacturer	Meraki
Local exhaust	☑
NAS-IP-Address	

Confirm

UCOPIA CONFIGURATION

Create a portal association on the concerned zone (e.g. « Meraki »):



Portals

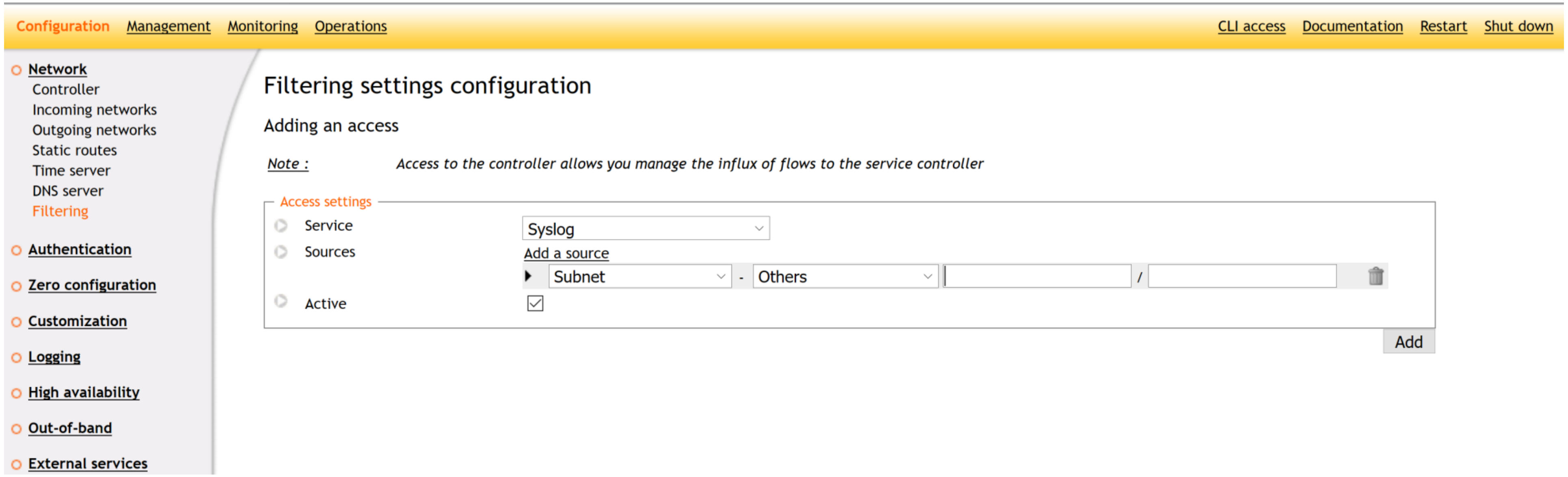
Adding an association to an incoming zone

Association settings

Zone	Meraki
Captive portal configuration	TEST
Automatic connection configuration	No configuration
Mobile application configuration	No configuration
Delegation portal configuration	No configuration
Visual model	default
Active	☑

UCOPIA CONFIGURATION

Create a filtering access for UCOPIA syslog server to the different Cloud Meraki subnets listed above.



Filtering settings configuration

Adding an access

Note : *Access to the controller allows you manage the influx of flows to the service controller*

Access settings

Service: Syslog

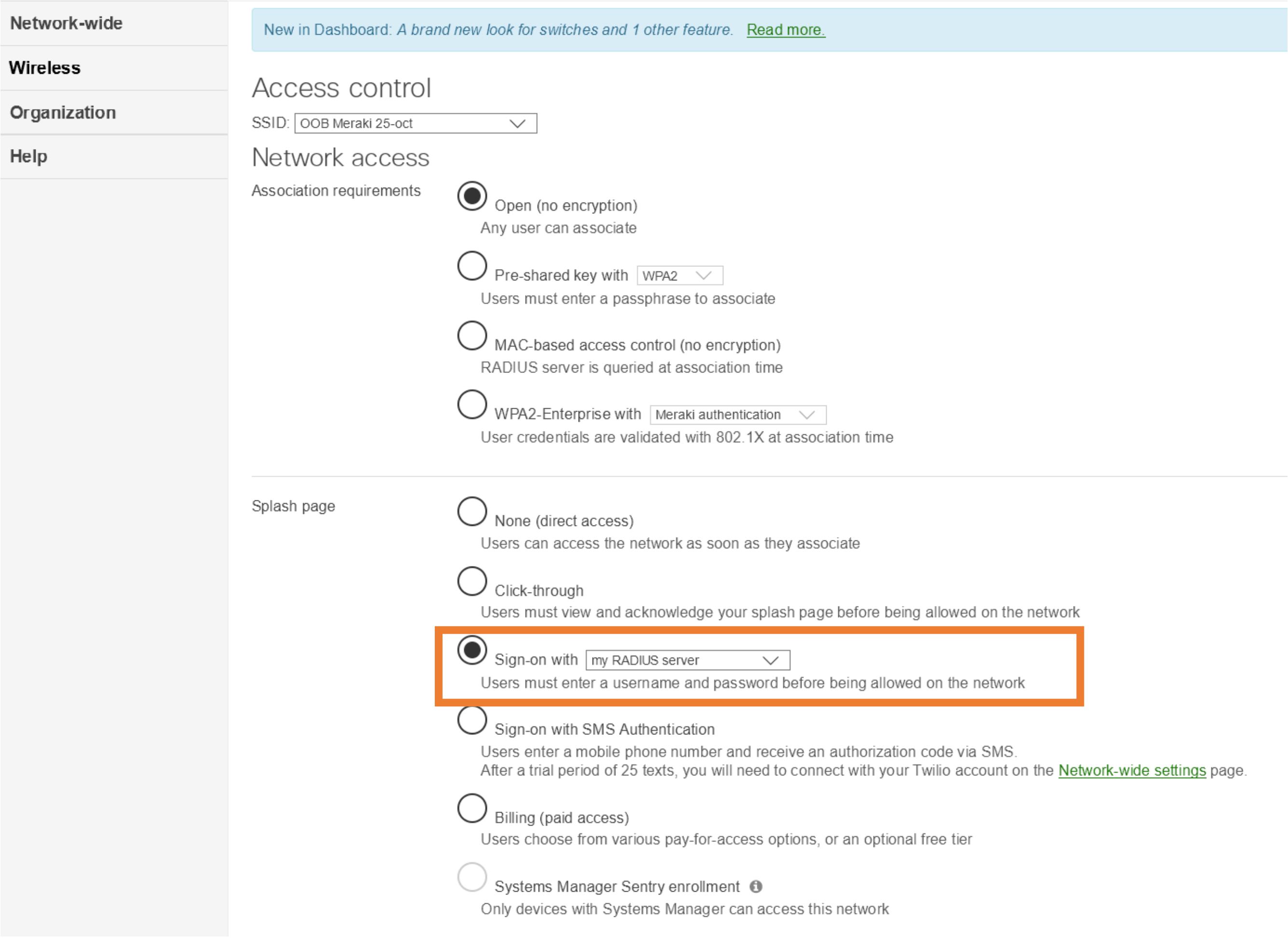
Sources: Add a source

Subnet - Others /

Active ☑

MERAKI CONFIGURATION

In « Wireless > Configure > Access control » of the concerned SSID (1/3):



New in Dashboard: *A brand new look for switches and 1 other feature.* Read more.

Access control

SSID: OOB Meraki 25-oct

Network access

Association requirements

● Open (no encryption)
Any user can associate

○ Pre-shared key with WPA2
Users must enter a passphrase to associate

○ MAC-based access control (no encryption)
RADIUS server is queried at association time

○ WPA2-Enterprise with Meraki authentication
User credentials are validated with 802.1X at association time

Splash page

○ None (direct access)
Users can access the network as soon as they associate

○ Click-through
Users must view and acknowledge your splash page before being allowed on the network

● Sign-on with my RADIUS server
Users must enter a username and password before being allowed on the network

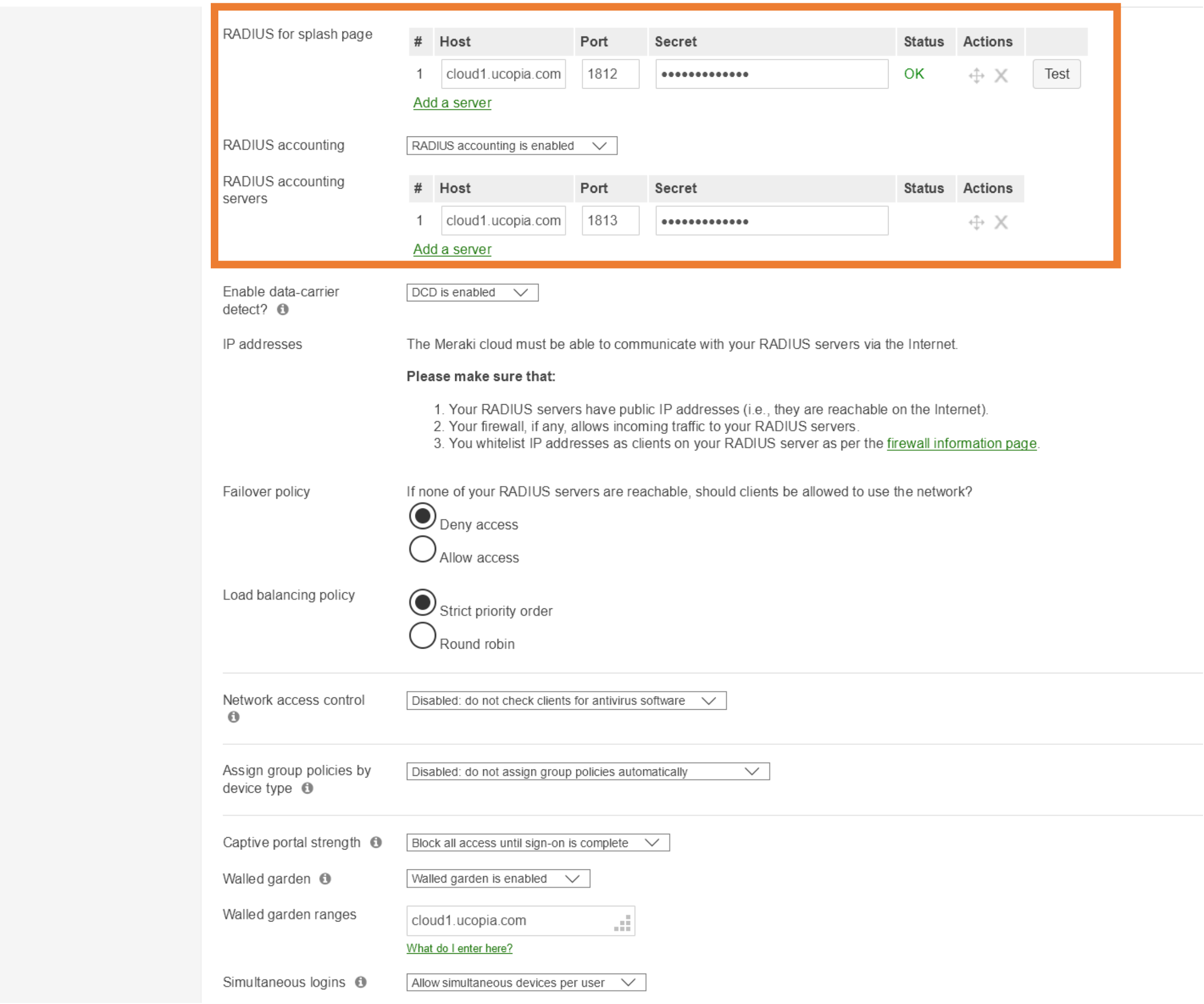
○ Sign-on with SMS Authentication
Users enter a mobile phone number and receive an authorization code via SMS.
After a trial period of 25 texts, you will need to connect with your Twilio account on the Network-wide settings page.

○ Billing (paid access)
Users choose from various pay-for-access options, or an optional free tier

○ Systems Manager Sentry enrollment
Only devices with Systems Manager can access this network

MERAKI CONFIGURATION

In « Wireless > Configure > Access control » of the concerned SSID (2/3):



RADIUS for splash page

#	Host	Port	Secret	Status	Actions	
1	cloud1.ucopia.com	1812	•••••••••••••	OK	✣ ✕	Test

Add a server

RADIUS accounting: RADIUS accounting is enabled

RADIUS accounting servers

#	Host	Port	Secret	Status	Actions
1	cloud1.ucopia.com	1813	•••••••••••••		✣ ✕

Add a server

Enable data-carrier detect? ℹ: DCD is enabled

IP addresses: The Meraki cloud must be able to communicate with your RADIUS servers via the Internet.

Please make sure that:

1. Your RADIUS servers have public IP addresses (i.e., they are reachable on the Internet).
2. Your firewall, if any, allows incoming traffic to your RADIUS servers.
3. You whitelist IP addresses as clients on your RADIUS server as per the firewall information page.

Failover policy: If none of your RADIUS servers are reachable, should clients be allowed to use the network?

● Deny access

○ Allow access

Load balancing policy:

● Strict priority order

○ Round robin

Network access control ℹ: Disabled: do not check clients for antivirus software

Assign group policies by device type ℹ: Disabled: do not assign group policies automatically

Captive portal strength ℹ: Block all access until sign-on is complete

Walled garden ℹ: Walled garden is enabled

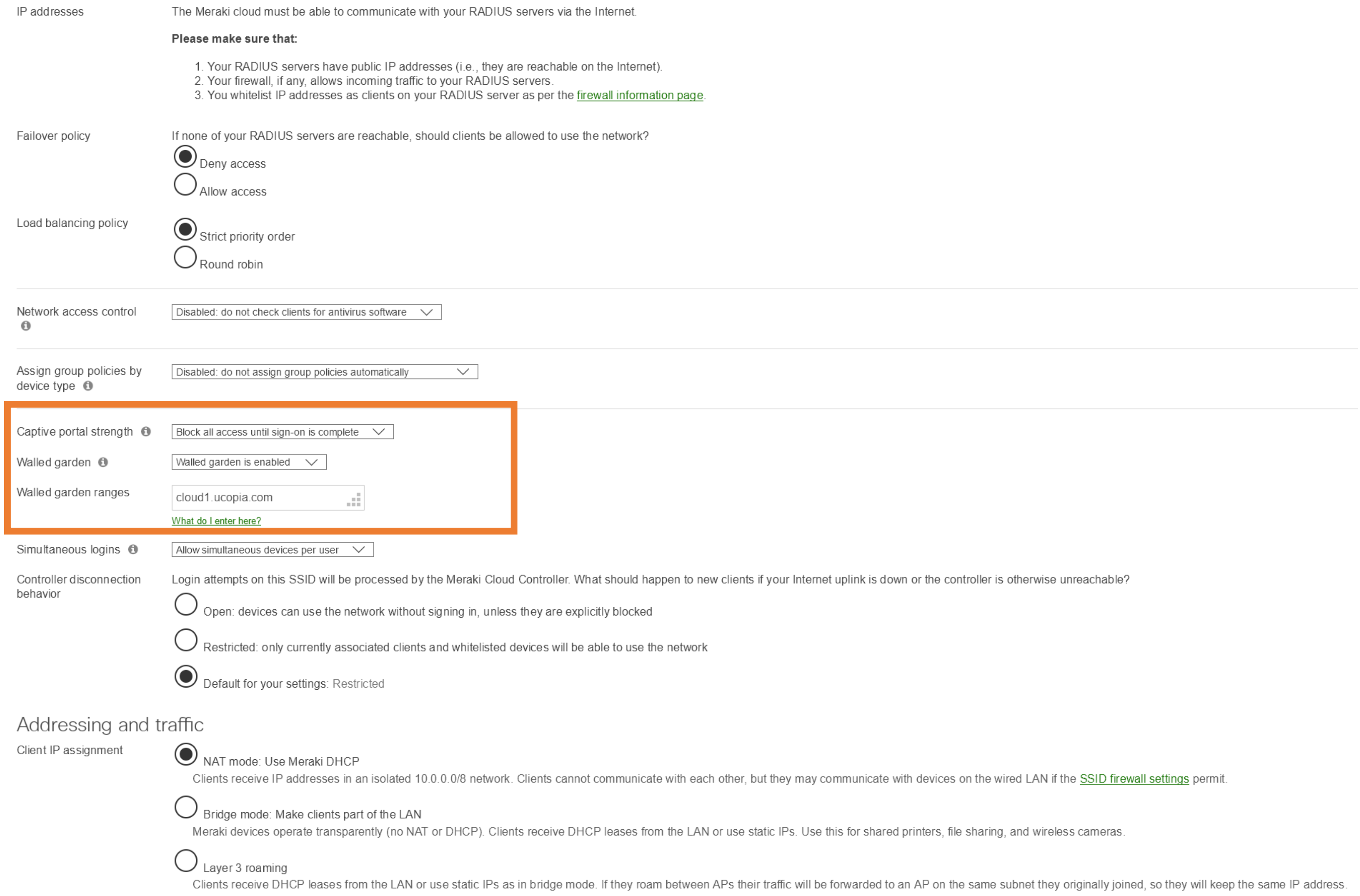
Walled garden ranges: cloud1.ucopia.com

What do I enter here?

Simultaneous logins ℹ: Allow simultaneous devices per user

MERAKI CONFIGURATION

In « Wireless > Configure > Access control » of the concerned SSID (3/3):



IP addresses — The Meraki cloud must be able to communicate with your RADIUS servers via the Internet.

Please make sure that:

1. Your RADIUS servers have public IP addresses (i.e., they are reachable on the Internet).
2. Your firewall, if any, allows incoming traffic to your RADIUS servers.
3. You whitelist IP addresses as clients on your RADIUS server as per the firewall information page.

Failover policy — If none of your RADIUS servers are reachable, should clients be allowed to use the network?

● Deny access
○ Allow access

Load balancing policy

● Strict priority order
○ Round robin

Network access control: Disabled: do not check clients for antivirus software

Assign group policies by device type: Disabled: do not assign group policies automatically

Captive portal strength: Block all access until sign-on is complete

Walled garden: Walled garden is enabled

Walled garden ranges: cloud1.ucopia.com

What do I enter here?

Simultaneous logins: Allow simultaneous devices per user

Controller disconnection behavior — Login attempts on this SSID will be processed by the Meraki Cloud Controller. What should happen to new clients if your Internet uplink is down or the controller is otherwise unreachable?

○ Open: devices can use the network without signing in, unless they are explicitly blocked
○ Restricted: only currently associated clients and whitelisted devices will be able to use the network
● Default for your settings: Restricted

Addressing and traffic

Client IP assignment

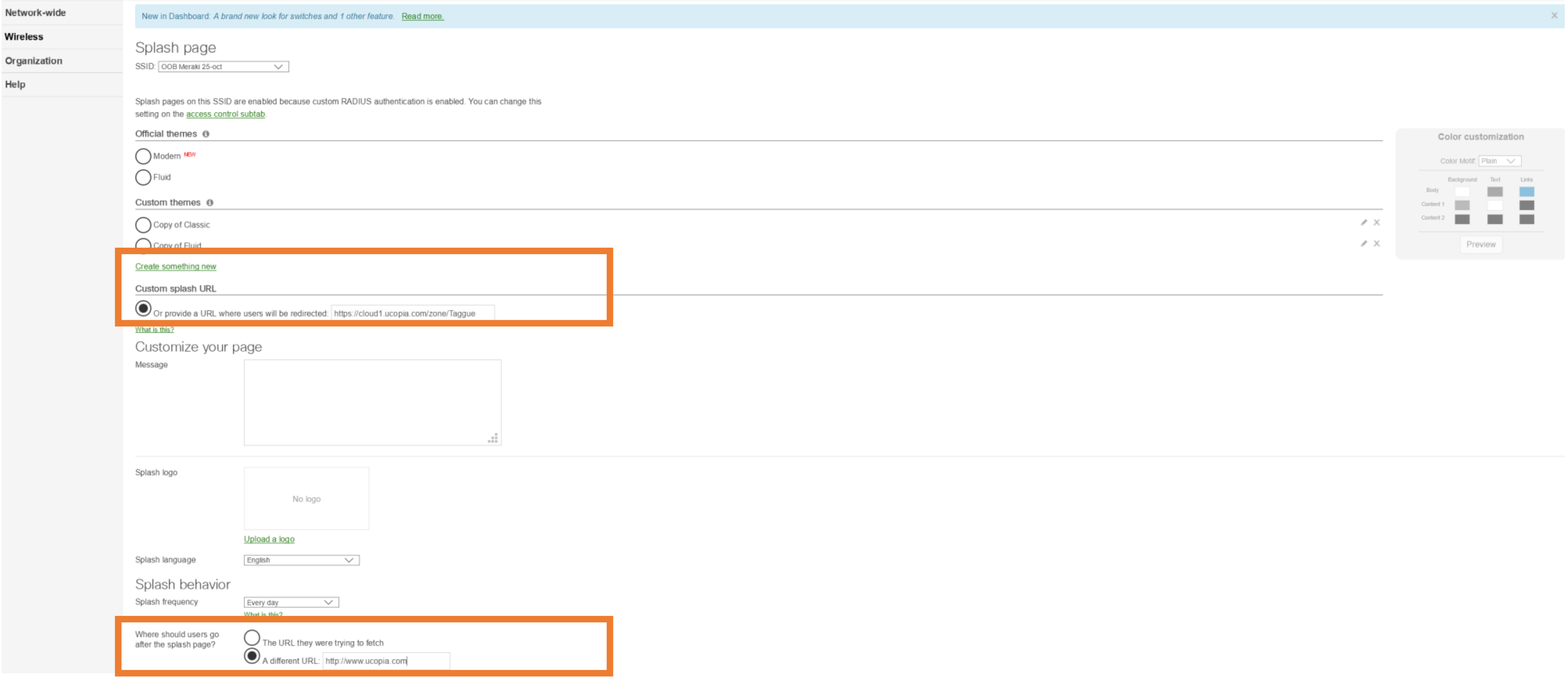
● NAT mode: Use Meraki DHCP
Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the SSID firewall settings permit.

○ Bridge mode: Make clients part of the LAN
Meraki devices operate transparently (no NAT or DHCP). Clients receive DHCP leases from the LAN or use static IPs. Use this for shared printers, file sharing, and wireless cameras.

○ Layer 3 roaming
Clients receive DHCP leases from the LAN or use static IPs as in bridge mode. If they roam between APs their traffic will be forwarded to an AP on the same subnet they originally joined, so they will keep the same IP address.

MERAKI CONFIGURATION

In « Wireless > Configure > Splash page » of the concerned SSID:



New in Dashboard: *A brand new look for switches and 1 other feature.* Read more.

Splash page

SSID: OOB Meraki 25-oct

Splash pages on this SSID are enabled because custom RADIUS authentication is enabled. You can change this setting on the access control subtab.

Official themes

○ Modern NEW

○ Fluid

Custom themes

○ Copy of Classic

○ Copy of Fluid

Create something new

Custom splash URL

● Or provide a URL where users will be redirected: https://cloud1.ucopia.com/zone/Taggue

What is this?

Customize your page

Message

Splash logo

No logo

Upload a logo

Splash language: English

Splash behavior

Splash frequency: Every day

What is this?

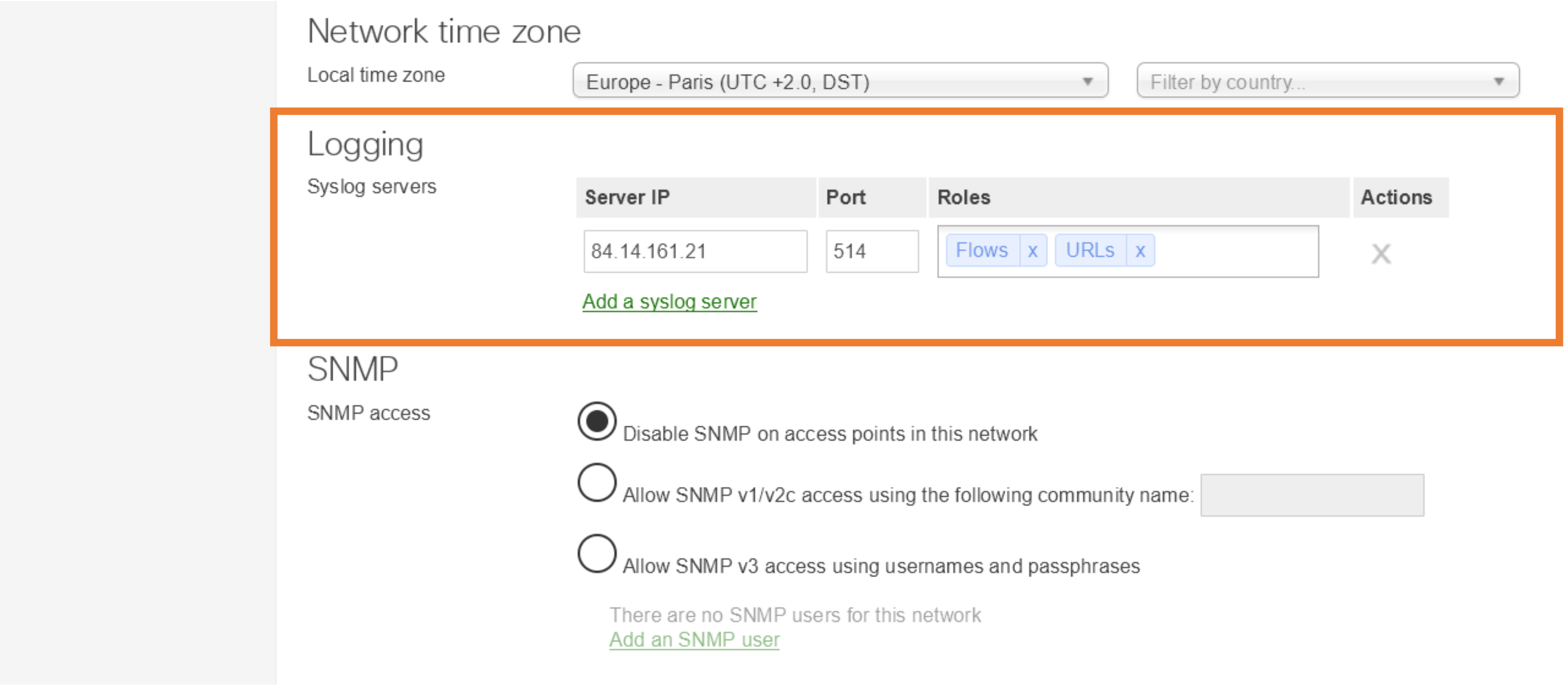
Where should users go after the splash page?

○ The URL they were trying to fetch

● A different URL: http://www.ucopia.com

MERAKI CONFIGURATION

In « Network-wide > Configure > General »:



Network time zone

Local time zone: Europe - Paris (UTC +2.0, DST) ▾ | Filter by country... ▾

Logging

Syslog servers

Server IP	Port	Roles	Actions
84.14.161.21	514	Flows x URLs x	×

Add a syslog server

SNMP

SNMP access

● Disable SNMP on access points in this network

○ Allow SNMP v1/v2c access using the following community name:

○ Allow SNMP v3 access using usernames and passphrases

There are no SNMP users for this network

Add an SNMP user